AFFIDAVIT IN SUPPORT OF APPLICATIONS FOR SEARCH WARRANTS

I, Jason J. DeFreitas, being duly sworn, depose and state as follows:

1. I am a Special Agent with the Department of Homeland Security Immigration and Customs Enforcement, Homeland Security Investigations ("HSI"). I am assigned to the Boston Field Office and have been employed by HSI since 2006. Prior to my assignment to the Boston Field Office, I was assigned to the HSI Los Angeles Field Office, where I served as a member of the Intellectual Property Rights Group. I am currently assigned to the Cyber Group.

2. In connection with my official duties, I have investigated and assisted other agents in investigating cases involving a wide variety of criminal violations including, but not limited to, fraud, intellectual property rights, cultural property theft, and child pornography. Prior to my employment with HSI, I served as a Customs and Border Protection Officer at the Los Angeles International Airport for approximately four years. My duties included the interception and examination of individuals and merchandise for violations of United States laws.

3. On July 30, 2020, I was involved in the arrest of Michael D. Irons ("IRONS"), born 1976. IRONS was arrested for possession of child pornography, in violation of 18 U.S.C. § 2252A(a)(5)(B).

PURPOSE OF AFFIDAVIT

4. This affidavit is made in support of an application for a search warrant, under 18 U.S.C. § 2703(a) and Rule 41 of the Federal Rules of Criminal Procedure, to search and seize the Snapchat user account "Fun_boy1313" ("Snapchat Account"), and other data associated with this particular account, as described in Attachment A. There is probable cause to believe that the Snapchat Account contains the fruits, evidence, or instrumentalities of the receipt and possession of child pornography, in violations of 18 U.S.C. §§ 2252A(a)(2) and 2252A(a)(5)(B),

respectively (collectively, the "Subject Offenses"), as described in Attachment B.

5. The Snapchat Account and relevant data is stored at the premises owned, maintained, and operated by Snap Inc., a company headquartered at 2772 Donald Douglas Loop North, Santa Monica, California 90405, which functions as an electronic communications service and remote computing service, and is a provider of electronic and remote computing services.

6. The statements in this affidavit are based in part on information provided by other law enforcement officers and on my investigation of this matter. Since this affidavit is being submitted for the limited purpose of securing a search warrant, I have not included each and every fact known to me concerning this investigation.

INFORMATION REGARDING SNAPCHAT

7. Snapchat is a multimedia messaging and social media mobile application managed by Snap Inc., which allows users to share images, videos, and chat messages. During the account registration process, Snapchat asks subscribers to provide basic personal information, including email address, telephone number, and date of birth. Snapchat requires new users to create a username, which will be the unique identifier for the account and cannot later be changed.

8. One distinct feature of Snapchat is that the application allows users to place time restrictions on shared files, so that the images, videos or messages are only available to the recipient(s) for a short period of time before they become inaccessible. "Snaps" are photos or videos taken using the Snapchat application's camera on a user's mobile device, and may be shared directly with the user's friends, or in a "Story." A Story is a collection of Snaps displayed in chronological order. Users can share a Story with their friends, a customized recipient list, or with all Snapchat users.

9. The company processes approximately 700 million snaps every day. Snapchat users access the application frequently. According to marketing material provided by the company, the average Snapchat user checks their account 14 times per day.

10. "Memories" is a cloud-storage service provided by Snapchat, which allows users to save their Snaps (sent or unsent) and Stories, as well as images and videos from their mobile device. Content saved in Memories is stored on Snapchat's servers until deleted by the user. Snapchat allows users to encrypt their content stored in Memories, and these files are called "My Eyes Only" files. My Eyes Only content is reportedly accessible to Snapchat employees, but cannot be decrypted by the company without the user's password.

11. Another feature available to Snapchat users is the "Chat" feature. A user can type messages and send photos, videos, audio notes, and video notes to friends within the Snapchat application. Once a chat message is viewed by both the sender and the recipient, and both parties swipe away from the chat screen, the message will be cleared. Within the Snapchat application itself, a user can opt to save part of the chat by tapping on the message that they want to keep. The user can clear the message by tapping it a second time.

12. Snapchat retains logs for Snaps for thirty days. Logs for posted Stories are retained for 24 hours or until deleted by the user. Chat content will be available only if the sender or the recipient chooses to save the Chat, or if the Chat is unopened (within thirty days of sending). Memories may be available until deleted by the user.

13. While a Snapchat message may disappear, the record of who sent it and when still exists. Snapchat records and retains information that is roughly analogous to the call detail records maintained by telecommunications companies. This includes the date, time, sender, and recipient of a snap. Additionally, Snapchat stores the number of messages exchanged, which

users they communicate with the most, message status including if and when the message was opened, and whether the receiver used the native screen capture function of their device to take a picture of the snap before it disappeared.

14. Based on my training and experience in child exploitation investigations, I am aware that Snapchat stores and maintains electronic communications and data relating to subscribers of their services. This information includes basic subscriber information, account access information, shared content (for certain periods of time), and location data. This information may constitute evidence of the crimes under investigation as it may contain information that will identify the party in control of the suspect account.

15. On July 30, 2020, I submitted a letter requesting under 18 U.S.C § 2703(f) that the company preserve records associated with the Snapchat Account for a period of 90 days.

EVIDENCE IN SUPPORT OF PROBABLE CAUSE

16. This investigation began after HSI received a report from the online application Kik Messenger (hereinafter, "Kik"). Kik is a free instant messaging application for mobile devices used to transmit messages, images, videos, and other content. Prior to October 2019, Kik Interactive, Inc., a Canadian company, owned and operated Kik. After October 2019, MediaLab, Inc., a United States company, acquired Kik.[1]

17. Kik Messenger allows users to create a username without providing a telephone number or personally identifying information. After registering a username, KiK users can receive messages, photos, videos, sketches, mobile webpages, and other content.

[1] The information outlined in this affidavit regarding the suspect user was obtained from Kik before the company's American acquisition. However, the application's functionality remains substantially the same, as evidence by the below Kik's Guide for Law Enforcement, available at: https://help.kik.com/hc/en-us/articles/217681728-guide-for-Law-Enforcement.

18. In November 2019, I received a report from Kik dated July 5, 2019 regarding an individual with the Kik username "Fun_boy1313." According to the report, "Fun_boy1313" provided to Kik their name as "M D," their email address as "yomiketow@gmail.com," their phone type as Android, and their phone model as SM-G920P.

19. Through open-source resources, I know that SM-G920P is the model number for a Samsung Galaxy S6 phone manufactured for use on the Sprint network.

20. According to the report, "Fun_boy1313" used Kik to send three videos of child pornography. Kik was alerted to the videos of child pornography sent by "Fun_boy1313" on July 5, 2019 through an Abuse Report submitted by another user.

21. According to the July 5, 2019 Kik Report, the IP address associated with "Fun_boy1313" was 24.63.240.155. This IP address was used to send the three videos. A query within the American Registry for Internet Numbers ("ARIN") online database revealed that IP address 24.63.240.155 was registered to Comcast Communications ("Comcast").

22. On December 19, 2019, an administrative summons was issued to Comcast for the subscriber information associated with IP address 24.63.240.155 on July 5, 2019. Comcast returned the following information: 238 West Street, Gardner, Massachusetts 01440 (the "Subject Premises"). I further determined that IRONS resides at the Subject Premises and is employed by a towing company.

23. I reviewed the videos attached to the July 5, 2019 Kik Report and determined that two of the videos depict child pornography. On July 28, 2020, I obtained federal warrants authorizing the search of the Subject Premises and IRONS' person.

24. On July 30, 2020, HSI executed the search warrant on the Subject Premises. Agents found two phones in IRONS' bedroom. One phone was a Samsung Galaxy S6 ("S6"); the other phone was a Samsung Galaxy S9 ("S9").

25. IRONS agreed to speak to agents and confirmed that both phones described above belonged to him. IRONS further confirmed that "Fun_boy1313" was his username on Kik and admitted to trading, sharing, and distributing child pornography. IRONS stated that he used Kik as recently as the day before, July 29, 2020.

26. IRONS further stated that he would also use Snapchat. IRONS stated that after meeting underage girls on the Kik application, IRONS would continue the conversation on Snapchat. IRONS stated that he believed the girls he spoke to were as young as 15 years of age.

27. IRONS further stated that he would send to the girls naked pictures of himself in exchange for naked pictures of the girls.

28. IRONS further stated that he used cloud storage to retain the images of child pornography. Specifically, IRONS stated he used the application Mega[2] for that purpose and confirmed to agents that there was child pornography on his phones.

29. During a preliminary search of the S9 cell phone, HSI agents found approximately 300 videos, which according to the metadata, came from the Mega application. Of the 300 videos, agents believe that at least 150 videos contain child pornography. On the S6 phone, agents found at least 50 videos of child pornography.

30. Both phones also contained the Kik application. On both phones, the username associated with the application is "Fun_boy1313." In addition, the email address "yomiketow@gmail.com" is associated with the S9 cell phone.

[2] Mega is a cloud storage and file hosting application available for both Android and Apple devices.

31. HSI agents also found the Snapchat application on the S6 and S9 cell phones. The username associated with the Snapchat application on both phones is "Fun_boy1313." Specifically, on the S9 phone, the Snapchat application was still logged in the "Fun_boy1313" account.

LEGAL AUTHORITY

32. The government may obtain both electronic communications and subscriber information by obtaining a search warrant. 18 U.S.C. §§ 2703(a), 2703(c)(1)(A).

33. Any court with jurisdiction over the offense under investigation may issue a search warrant under 18 U.S.C. § 2703(a), regardless of the location of the Internet company whose information will be searched. 18 U.S.C. § 2703(b)(1)(A). Furthermore, unlike other search warrants, § 2703 warrants do not require an officer to be present for service or execution of the search warrant. 18 U.S.C. § 2703(g).

34. If the government obtains a search warrant, there is no requirement that either the government or the provider give notice to the subscriber. 18 U.S.C. §§ 2703(b)(1)(A), 2703(c)(3).

FOURTEEN-DAY RULE FOR EXECUTION OF THE WARRANT

35. Federal Rule of Criminal Procedure 41(e)(2)(A),(B) directs the United States to execute a search warrant for electronic evidence within 14 days of the warrant's issuance. If the Court issues this warrant, the United States will execute it not by entering the premises of Snap, Inc., as with a conventional warrant, but rather by serving a copy of the warrant on Snap, Inc. and awaiting its production of the requested data. This practice is approved in 18 U.S.C. § 2703(g), and it is generally a prudent one because it minimizes the government's intrusion onto internet companies' physical premises and the resulting disruption of their business practices.

36. Based on the training and experience of myself and other law enforcement, I understand that e-mail and social media providers sometimes produce data in response to a search warrant outside the 14-day (formerly 10-day) period set forth in Rule 41 for execution of a warrant. I also understand that electronic communication companies sometimes produce data that was created or received after this 14-day deadline ("late-created data"). The United States does not ask for this extra data or participate in its production.

37. Should Snap, Inc. produce late-created data in response to this warrant, law enforcement personnel will seek to avoid reviewing any late-created data that was created by or received by the account-holder absent a follow-up warrant. However, I request permission to view all late-created data that was created by Snap, Inc., including subscriber, IP address, logging, and other transactional data, without a further order of the Court. This information could also be obtained by grand jury subpoena or an order under 18 U.S.C. § 2703(d), neither of which contains a 14-day time limit.

38. For these reasons, I request that the Court approve the procedures detailed in the Attachment B, which sets forth these limitations.

INFORMATION TO BE SEARCHED AND THINGS TO BE SEIZED

39. I anticipate executing this warrant under the Electronic Communications Privacy Act, in particular Title 18, United States Code, Sections 2703(a), 2703(b)(1)(A) and 2703(c)(1)(A), by using the warrant to require the Snap Inc. to disclose to the government copies of the records and other information (including the content of the communications) particularly described in Section I of Attachment B. Upon receipt of the information described in Section I of Attachment B, government-authorized persons will review that information to locate the items described in Section II of Attachment B.

CONCLUSION

40. Based on the information described above, there is probable cause to believe that Michael D. Irons has committed the Subject Offenses.

41. Based on the information described above, there is also probable cause to believe that the Snapchat Account (as described in Attachment A) contains fruits, evidence, or instrumentalities of these crimes (as described in Attachment B). The procedures for copying and reviewing the relevant records are set out in Attachment B.

42. I further request that the Court direct Snap, Inc. to disclose to the government any information described in Section I of Attachment B that is within its possession, custody, or control. Because the warrant will be served on Snap, Inc., who will then compile the requested records at a time convenient to it, reasonable cause exists to permit the execution of the requested warrant at any time in the day or night.

Sworn to under the pains and penalties of perjury,

Special Agent Jason J. DeFreitas
Homeland Security Investigations

Time and Date: **Aug 6, 2020** 3:50 p.m.

Notice is hereby provided that, pursuant to Federal Rule of Criminal Procedure 4.1, the affiant was sworn by telephone on the date and time indicated above and on the search warrants issued by the Court.

Honorable David H. Hennessy
United States Magistrate Judge

CERTIFICATE OF AUTHENTICITY OF DOMESTIC BUSINESS RECORDS PURSUANT TO FEDERAL RULE OF EVIDENCE 902(11)

I, _____, attest, under penalties of perjury under the laws of the United States of America pursuant to 28 U.S.C. § 1746, that the information contained in this declaration is true and correct. I am employed by Snap, Inc., and my official title is _____. I am a custodian of records for Snap, Inc.. I state that each of the records attached hereto is the original record or a true duplicate of the original record in the custody of Snap, Inc., and that I am the custodian of the attached records consisting of _____ (pages/CDs/kilobytes). I further state that:

a. all records attached to this certificate were made at or near the time of the occurrence of the matter set forth, by, or from information transmitted by, a person with knowledge of those matters;

b. such records were kept in the ordinary course of a regularly conducted business activity of Snap, Inc.; and

c. such records were made by Snap, Inc. as a regular practice.

I further state that this certification is intended to satisfy Rule 902(11) of the Federal Rules of Evidence.

_____ _____

Date Signature